FORSCOM Pamphlet 25-25

Headquarters, United States Army Forces Command
1777 Hardee Avenue, SW
Fort McPherson, GA 30330-1062
15 May 2005

Information Management

Information Technology User's Guide

Summary. This pamphlet is a guide to using information technology (glossary) in the workplace. In support of information assurance, this guide prescribes procedures for using Government computers in a way that protects them against viruses and hackers.

Summary of Change. This is a new policy incorporating Department of Defense and Army information assurance policy.

Applicability. This pamphlet applies to military, contractors and civilian personnel in US Army Forces Command (FORSCOM) who use Government computers in the workplace, at home or when traveling.

Forms. FORSCOM and higher-level forms are available through the Directorate of Information Management, Forest Park, GA. Ordering information is available on the FORSCOM web site at FORSCOM Pam 25-30

Records Management. Records created as a result of processes prescribed by this pamphlet must be identified, maintained, and disposed of according to AR 25-400-2, The Army Records Information Management System, 15 November 2004. Record titles and descriptions are available on the Army Records Information Management System web site at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this pamphlet is the Deputy Chief of Staff, G-6. Users are invited to send comments and suggestions on DA Form 2028, Recommended Changes to Publications and Blank Forms, to CDR, FORSCOM, AFCI-IC, 1777 Hardee Avenue, SW, Fort McPherson, GA 30330-1062.

Changes. Changes to this pamphlet are not official unless authenticated by the FORSCOM G-6.

Distribution restrictions. Approved for public release; distribution unlimited. Local reproduction is authorized.

FOR THE COMMANDER:

DAN K. MCNEILL
General, USA
Commanding

OFFICIAL:

//SIGNED//
WILLIAM T. LASHER
Colonel, GS
Deputy Chief of Staff, G-6

DISTRIBUTION of this pamphlet is special, whereas, copies should be furnished to the lowest command levels of the Active Army, Army National Guard and US Army Reserve.

Copies furnished:
US Army Garrison (IMSE-MPH-HRS) (record copy).

TABLE OF CONTENTS

1. Purpose

a. This pamphlet is intended to familiarize users of the FORSCOM Command and Control System (FCCS) with procedures for computer use, security, and care.

b. As a user of a Government computer, you can greatly affect the security of our networks. Protecting the information on those networks is called information assurance. This guide will help you protect our networks and information by showing you how to recognize and avoid the hazards and increasingly sophisticated threats to our networks.

c. Before you can be issued a license to "drive," on FORSCOM networks, you must take the Computer-User Test (paragraph 7.a(g)) and sign the Computer-User Agreement (Appendix A). This agreement is your promise to use the network responsibly and to follow the command policy on computer use. This guide tells you everything you need to know to pass the test.

2. FORSCOM Command and Control System – General Overview

a. The FCCS comprises individual workstations (computers) for employees use, standard office and Command and Control software, local area networks (LAN) that allow systems to communicate, and servers that provide electronic mail (e-mail), database, and other mission services. FCCS has two separate LAN enclaves:

(1) The unclassified portion of the FCCS is part of Department of Defense's (DOD's) overall Non-secure Internet Protocol Router Network (NIPRNet). Use of this network is limited to unclassified and For Official Use Only materiel. Users MUST NOT process or introduce any classified materiel onto the NIPRNet. This portion of the FCCS is connected to the greater commercial internet and "world-wide web" through equipment designed to reduce vulnerabilities by external threats. Security measures on the part of each user are PARAMOUNT to the defense of this network. You will find a large portion of this manual addresses measures each user must follow to keep our network secure.

(2) The classified portion of the FCCS is part of DOD's Secure Internet Protocol Router Network (SIPRNet), a network that is physically and electronically isolated from both the NIPRNet and the Internet. Use of this network is limited to material classified at the collateral SECRET classification and below. Under NO circumstances must users introduce material which is SCI or classified above SECRET onto this network.

b. Organization. The FCCS is operated primarily by the Information Technology Services Division within the FORSCOM G-6. Each primary FORSCOM Directorate has an Information Management Officer (IMO) assigned to handle directorate-level automation requirements. The FCCS maintains a 24-hour help desk in the basement of building 200, Fort McPherson (404-464-2222) to assist users with automation questions or problems. When practical, users should go through their respective IMO before calling or visiting the help desk.

c. Hardware. User's computers (workstations) are available in standard desktop and laptop configurations based on hardware available through Army-level contracts. Speed and capability of individual machines will vary based primarily on the age of the equipment. Replacement or upgrade of hardware is done as resources become available to allow "technology refresh." Otherwise, hardware is not generally upgraded unless required specifically by mission. Unique hardware devices or configurations generally result in substantially higher maintenance costs and will not be permitted unless necessary to support a specific mission. All requests for hardware will be submitted to directorate IMOs.

d. Software. Each user workstation is loaded with a baseline of standard office automation, internet, and e-mail software for general use. Software on FCCS machines must be government owned and authorized for use by proper authorities. Unique software will be permitted only if specifically required for mission support and if properly acquired, licensed, and tested by FCCS engineers. Appendix B lists standard software available for unclassified and classified machines. Requests for software not included in the baseline should be submitted through directorate IMOs.

e. Access to FCCS. Authorized users may apply for and be issued FCCS accounts after becoming familiar with this manual, passing the FCCS Computer-User Test and signing the Computer-User Agreement.

(1) Applying for FCCS accounts (In-processing):

(a) Each individual requiring access to the FCCS networks must in-process starting with their Directorate IMO. The IMO and directorate Security Officer will validate the user's clearance and submit a HQ FORSCOM 650-E requesting account (s) for the user and the appropriate access to Directorate resources.

(b) The FCCS Information Assurance Security Office (IASO) will verify the user has passed the Computer-User Test and signed the Computer-User Agreement.

(c) With a passing grade and signed agreement, the user's account (s), user name and passwords will be issued and their accounts activated.

(2) Out-processing. Users permanently departing FORSCOM will notify their IMO they are out-processing and the IMO will submit a HQ FORSCOM Form 650-E requesting their account (s) be deleted.

(a) The FCCS IASO will delete the account (s) on the user's departure date.

(b) User's e-mail accounts will be hidden from view on the servers and deleted after 60 days.

(3) Moving within the command. If a user is moved to a position in another agency or Directorate on the FCCS network, the user must notify their IMO. The losing IMO will submit a HQ FORSCOM Form 650-E annotating the move. The gaining IMO will also submit a HQ FORSCOM Form 650-E annotating the changes needed in the user's account permissions.

f. Training. The FORSCOM G-6 offers periodic training courses on specialized Army and DOD applications, to include the Global Command and Control System (GCCS) and the Defense Message System (DMS/AMHS). Appendix C lists specific training courses available and contact information for latest course schedules.

3. Your Government Computer as a Gateway to Information and the Internet

a. Since almost all unclassified computers in the FCCS are networked, your computer can reach or be reached by almost every unclassified computer in DOD. Because other DOD computers trust your computer, you have access to DOD information not available to the general public. Additionally, almost all computers on the NIPRNet are linked to the commercial Internet. The SIPRNet, although not linked to the commercial Internet, is used to link DOD computers together to share information classified up to Secret.

b. This internetworking of computers makes your computer a gateway to vast amounts of information. It also exposes your computer to risks from all computers to which it can be linked. As a user of a computer on the FCCS, you play a key role in protecting our data. It is imperative you understand and follow the guidelines for computer security prescribed in paragraph 6.

4. Use of Your Government Computer

a. Safeguarding Government Computers.

(1) The computer you are using is the property of the US Government. Government computers are to be used by Government employees for official business, authorized personal use, and limited morale and welfare communications between deployed soldiers and their family members. All users must—

(a) Safeguard each information system and its contents against sabotage, tampering, denial-of-service, espionage, and release to unauthorized persons.

(b) Protect hardware, software, and documentation at the highest classification of the information residing on the information system.

(c) Report information systems security incidents, vulnerabilities, and virus attacks to your Information Management Officer (IMO) or the FCCS Help Desk, (404) 464-2222.

(d) Check all removable media (for example: disks, compact disks (CDs), tapes, universal serial bus (USB) memory sticks) for malicious software (for example: viruses and worms) before using it on a computer, Information Technology (IT) system, and the FCCS.

(e) If your computer has been disconnected from the network for a week or more (for example: when taking your laptop computer home for work or returning from temporary duty), you must check with the FCCS Help Desk to ensure that the system complies with the latest Information Assurance Vulnerability Alert (IAVA) prior to re-connecting to the network.

(f) Physical Security of Laptops. Whenever possible, laptop computers will be maintained under the direct supervision of the user. Users should exercise extra precautionary security measures when laptops are taken from the workplace.

(2) Soldiers who fail to comply with this policy may be subject to adverse administrative action or punishment under Article 92 of the UCMJ. Personnel not subject to the UCMJ may be subject to adverse action under the United States Code or Federal regulations.

b. Authorized Personal Use. Authorized personal use is defined by the Joint Ethics Regulation (JER) (DOD Reg 5500.7), paragraph 2-301, and AR 25-1, Army Knowledge Management and Information Technology Management, 30 June 2004. This use includes brief access to, searches on the Internet, and sending personal e-mail messages. The JER also requires commanders and supervisors to ensure that personal use of computers does not adversely affect the performance of official duties. Personal use of computers is authorized when it—

(1) Conforms to DOD, Department of the Army and FCCS policies.

(2) Is of reasonable duration and frequency and, when possible, is done before or after normal duty hours.

(3) Does not create significant additional costs to DOD or the Army, and does not reflect adversely on DOD or the Army.

(4) Serves a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare. Employees may also be allowed to conduct job searches in response to downsizing. Using government computers to allow deployed soldiers and their immediate family members to exchange email is authorized and encouraged.

(5) Supports your personal and private participation in appropriate non-federal and not-for-profit professional organizations (see JER 3-211, paragraphs 3-300b and 3-305), subject to supervisor approval and the limitations above.

(6) Does not overburden the military communication system. Remember, the military communication system (of which the NIPRNet plays a vital part) is designed to support the mission requirements of the warfighter.

c. Passwords.

(1) Your password is your key to accessing FORSCOM networks. While this key opens the vast world of various military networks and the Internet, it can also allow others access to the same information. Each authorized FCCS user will be issued a unique log-on name and password for each computer account you use. Maintaining the security of your password is one of the most important security precautions you must take as a user. You alone are responsible for protecting your password and any e-mail messages that originate from your account. If someone obtains your password, they could assume your identity in the virtual world. You are responsible for any activity that takes place on a computer under your logon name and password. Do not share your password with anyone. The guidelines below will help you protect your password.

(a) Do not write down or post your password in your work area.

(b) Do not store your password online or in a PDA or PED, and do not include it in e-mail messages.

(c) Make sure your password is not exposed on the screen when you log in. FORSCOM computers are set up to "star-out" password characters – do not change this setting.

(d) Ensure your password is changed every 150 days on the NIPRNet and every 90 days on the SIPRNet (you will be prompted at each logon starting two weeks before a password change is due). If you know that your password has been compromised, report it to your IMO/IASO and change it immediately.

(e) If your account is on a classified network, your password is classified at the highest level of information on that network, and you must protect it in the same manner as all classified information.

(2) Your password can be either user-generated or issued by your IASO. The following standards apply on the FCCS:

(a) User-generated: Passwords must have at least ten (10) characters and include at least two (2) uppercase letters, two (2) lowercase letters, two (2) numbers, and two (2) special characters. Special characters are the non alpha-numeric characters on the keyboard, such as ! @ # $ % ^ & and so forth. Passwords must not form a word or repeat any of your last ten (10) passwords. If your password does not meet current FCCS standards, you should change it immediately.

(b) IASO-generated and -issued: Passwords will be random, ten (10)-character, alpha numeric codes which meet all criteria above.

(3) Locked Out of System: The system will lock out and prohibit the user from logging onto his/her account after three failed attempts. This is a security measure to prohibit unauthorized access to your account. If your account is locked, contact the FCCS Help Desk to request your account to be unlocked. You will be required to verify and authenticate your identity before the SA resets your account.

(4) Never leave your computer unattended while logged on unless it is locked (Ctrl/Alt/Del) or protected by a "password protected" screensaver.

d. Use of the SIPRNet.

(1) Security of the SIPRNet (DOD's classified network) is of utmost importance. A vulnerability anywhere on the SIPRNet can lead potentially to significant compromise of information and damaging to US interests. Each user of the SIPRNet MUST maintain rigorous vigilance to ensure access to this network and protection of all information on it is restricted only to those with the proper security clearance and need to know.

(2) Any computer connected to the SIPRNet operates in the US Secret, "system-high" mode. Any removable media used on the system and printed output must be marked and controlled immediately according to AR 380-5, Department of the Army Information Security Program, 29 September 2000, until the data is declassified or downgraded by an approved process. In other words, writable disks or USB drives inserted into a Secret system are now considered Secret media and must be handled accordingly. A "Secret" label must be placed on classified media.

(3) You should not enter information into a system if the information—

(a) Has a higher classification than that for which the system is rated.

(b) Is proprietary, contractor-excluded, or otherwise needs special protection or handling.

(4) If a system is connected to the SIPRNet, only personnel with a US Secret or above security clearance will be allowed unescorted access to the system. Removable media, including CDs, disks, USB drives, or diskettes must not be removed from the computer area without the approval of the IMO/IASO. The IASO should inform you of TEMPEST - secure communication and data processing device requirements. TEMPEST (emissions security requirements) requires that classified system components be physically separated from unclassified components to prevent unauthorized emissions monitoring. For this reason, the movement of hardware and other IT equipment must be approved by your IASO or IMO.

(5) Uncleared personnel will not have access to areas where SIPRNet equipment is located. If an uncleared person is authorized access to a controlled area, he or she must be announced and escorted at all times, and computer screens must be covered. If an uncleared person is permitted to view a screen, US personnel must ensure that the information viewed is releasable to that individual. At no time will an uncleared person have control of a SIPRNet terminal.

(6) Unclassified information may be transferred from either the NIPRNet or SIPRNet, using a procedure called "air-gapping" (copying files to removeable media and transferring to systems of a higher or lower security

classification). See your FCCS IASO for approved procedures. Users will not perform air-gapping without written authorization.

e. Authorized Software and Hardware. Software and hardware used on any DOD computer must be licensed, accredited and approved by your Designated Approving Authority (DAA), IASO and IMO. You should store original software in a secure location, such as a locked cabinet or drawer. You may not load any software on your computer, install, or connect any hardware (including PDAs and PEDs, such as Palm Pilots) on the FCCS without first obtaining written approval from your DAA, IASO, System Administrator, or IMO. The DAA for the FCCS is the FORSCOM G-6. Users will inform their IASO and IMO of software requirements and obtain approval before installing software on a computer.

f. Personally-Owned Information Technology Equipment. Employee-owned IT resources (hardware and software) may be used to process Army-related work at the workplace provided the DAA approves it. All PDAs and PEDs (personal or Government-owned) must be loaded with DOD-approved, antivirus software.

g. Use of Army Knowledge Online (AKO). Soldiers, civilians, and contractors who are authorized e-mail accounts in FCCS are required to have an AKO web-mail account. All commercial web-mail services are prohibited for official Army business communications. AKO and FCCS also provide the only authorized Internet chat services allowed on the NIPRNet; all commercial chat services are prohibited. Each directorate will provide contractor civilians sponsorship for their AKO accounts.

h. Prohibited Web Sites. FCCS has implemented SmartFilter, which is a program that blocks users from accessing prohibited web sites (for example: those devoted to pornography and hate speech) and limits access for personal use. Authorized access may be obtained by exception. Contact your command IASO for assistance if you are blocked from a web site to which you legitimately require access.

i. Prohibited Activity. As a user, you are the first line of defense against unauthorized computer activity. The JER and FCCS policy define prohibited computer software and computer-network misbehavior. The following is a summary (not prioritized) of this policy and prohibited activity on computer networks:

(1) Having or loading prohibited software onto DOD computers. Prohibited software includes peer-to-peer file-sharing software, such as KaZaa, BitTorrent, Napster, Limeware, etc. (These services are commonly used to "share" Mpeg or MP3 music and video software); hacker tools and unauthorized development software; malicious logic and virus development software; unauthorized executables (files with an ".exe" extension), and macros; network line-monitoring and keystroke-monitoring tools; unlicensed (pirated) software; web-page-altering software; games (including "America's Army"); unmanaged personal firewalls (including DOD-licensed and Windows XP Internet connection firewalls); and any software not authorized by the DAA, IASO and IMO.)

(2) Using a commercial Internet chat service such as America Online (AOL) Instant Messenger, Yahoo Chat and web sites that promote chat services. The AKO and FCCS provide the only authorized chat services allowed on the NIPRNet.

(3) Personnel will employ government owned or provided e-mail systems or devices for government communications and the use of commercial ISP or e-mail accounts for official purposes is prohibited.

(4) Using networked IT or Government computers for personal gain or illegal activities.

(5) Attempting to strain, test, circumvent, or bypass computer-network or security controls.

(6) Attempting to access data or use operating systems or programs, except as specifically authorized.

(7) Performing network line-monitoring or keystroke-monitoring without proper authorization.

(8) Modifying or tampering with the software or hardware on your computer without the approval of your IASO and IMO.

(9) Moving your desktop computer without your IASO or IMO's approval. Most damage to computers occurs when moving them.

(10) Intentionally introducing viruses, worms, or malicious codes into any IT or network.

(11) Sharing user-identification or passwords.

(12) Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene material, such as racist, sexually explicit, harassing, or hate literature.

(13) Storing or processing classified information on a system (including PEDs and PDAs) not approved for classified processing.

(14) Storing or processing copyrighted material (including cartoons and music) unless approval is obtained from the author or publisher.

(15) Unauthorized viewing of changing, damaging, or deleting or blocking access to another user's files or communications.

(16) Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

(17) Giving an unauthorized individual access to a Government-owned or Government-operated system.

(18) Hacking into or from the FCCS network.

(19) Using someone else's user identification and password or masking your identity.

(20) Installing and using a modem without approval from your DAA.

(21) Writing or forwarding chain, jokes or hoax e-mail messages.

(22) Posting personal WebPages on FCCS.

(23) Using computers for personal profit.

(24) Downloading or loading freeware or shareware software.

(25) Simultaneously connecting to a Government network and a commercial ISP. (Users may connect to a commercial ISP then use a Virtual Private Network (VPN) to connect to the government network if the VPN software forces all network traffic through the VPN.)

(26) Simultaneously connecting to the NIPRNet and a commercial ISP with a PED or PDA modem.

(27) Posting of any work-related information on commercial web or Blog sites, newsgroups or forums.

j. Consent to Auditing and Monitoring.

(1) Auditing is defined as the independent review and examination of records and activities to assess the adequacy of system performance and controls, to ensure compliance with established policy and operational procedures, and to recommend necessary changes in controls, policy, or procedures. All transactions by users accessing the NIPRNet or SIPRNet are subject to audit.

(2) In general, Army members and employees use Government communications systems with the understanding that any type of use, authorized or unauthorized, incidental or personal, serves as consent to monitoring. When you click "OK" on the warning banner that appears when you start your computer, you are agreeing to have your computer monitored. Computers are monitored to ensure that use is authorized and that users follow security procedures. Among other things, monitoring is used for surveillance, to reconstruct account activity, and to record attempts to bypass security mechanisms.

k. Minimize Policy. During periods of heightened network activity, FCCS may be forced to minimize non--mission-essential activity on our networks. When a *MINIMIZE* order is issued to all users of FCCS, all personal use of networks is prohibited for the duration of the order, except for the following:

(1) E-mail messages between deployed soldiers and their families. Units are encouraged to make computers available to family support groups for supervised use of Government networks to exchange e-mail with soldiers deployed in support of contingency operations.

(2) Computer use required for Army or other authorized education center training or programs leading to college degrees.

l. Remote Access to FCCS. Several methods are available to access portions of the FCCS while away from the office. However, each of these requires strict adherence to stringent security procedures to avoid compromise of the information transmitted and the overall network.

(1) Security considerations for remote access.

(a) The only way to remotely access the FCCS SIPRNet is by using an authorized secure terminal connected directly to the SIPRNet.

(b) The most secure means to access the FCCS NIPRNet is to use an Army or DOD computer connected directly to the NIPRNet. This provides reasonable assurance the machine is compliant with security directives and will not pose a network threat.

(c) A personally owned computer may be used to remotely access FCCS-NIPR within the following guidelines:

- Personally owned systems must have active antivirus software with antivirus signature files not more than one week old. All current operating system security patches must be correctly applied. Remotely accessing FCCS with a computer that does not have the proper operating system patches and antivirus files will result in revocation of remote-access privileges.
- To get a current antivirus program, military and government civilians employees are encouraged to obtain a “Home Solution’s CD” from your IMO which includes DOD approved antivirus and firewall software, as well as various other useful programs authorized for home use.
- Government civilians and active-duty military personnel may also download and use antivirus and personal firewall software from ftp://ftp.cert.mil/pub/antivirus/home_use.htm (must download from .MIL domain). Authorized users can also download the retail version of McAfee VirusScan for Windows directly to their home system from http://www.mcafee.com/dod/.
- Users must configure their home systems to automatically download critical updates for Windows from Windows Update and configure antivirus software to automatically download virus signature updates daily to ensure the latest definitions are protecting the system.
- Users may not remotely connect to the FORSCOM network with any system which has peer-to-peer (P2P) software installed (for example: KaZaa, BearShare, Bittorrent, eDonkey, etc.). By its nature, P2P software shares portions of the user’s hard drive to the entire Internet, risking compromise of any data stored on the system. These programs also install hidden programs, which may include Trojan horse software, giving remote control of the system to a distant hacker. (Note if your personal computer is a general use computer accessible to other family members, YOU are responsible for ensuring they do not load peer-to-peer software on the machine).
- Users are responsible for ensuring any machine used for remote access complies with the standards above. IF YOU ARE NOT SURE ABOUT A MACHINE’S COMPLIANCE WITH THESE SECURITY DIRECTIVES, DO NOT USE IT TO REMOTELY ACCESS FCCS.

(d) Kiosk computers, such as those provided in hotel lobbies and public libraries are VERY LIKELY to be infected with key logging software which can capture the user’s login and password. These systems should not be trusted, and should not be used to read email.

(2) Outlook Web Access (OWA). Outlook web access is a web-based application which enables remote access to e-mail. It is available both on the NIPR and SIPR domains. OWA is the only remote access method

which will be available to users – other methods will require special approval. Any standard web browser can be used to view and manipulate OWA email given the proper web address (URL), userid and password.

(a) SIPRNet OWA. To access SIPRNet email you must use a DOD authorized secure terminal with access to the SIPRNet. Type in the URL for SIPR OWA, https://owa.force1.army.smil.mil/ and follow the onscreen instructions.

(b) NIPRNet OWA. NIPRNet Outlook Web Access is available at URL: https://owa.forscom.army.mil. Users reading their email via OWA MUST protect the government data from accidental release. Un-trusted computers should never be used to connect to OWA. When users finish reading email, it is critical they log out of OWA and close the browser window to prevent another person from walking up to the system and taking over the session. OWA does not store residual data on the local system (hard-drive) unless the user saves attachments. EMAIL ATTACHMENTS SHOULD NOT BE SAVED TO NON-GOVERNMENT COMPUTERS.

(3) FCCS Virtual Private Network (VPN). FCCS machines used for travel, such as laptops, may be authorized to have VPN installed. VPN software can be used to secure dial-up or high-speed internet connections to allow the user to operate as though connected directly to the FCCS NIPR network. VPN connections allow users to access most of the resources available to local users, to include shared drives and files. VPN accounts will only be issued to users with the proper equipment and a mission requirement. Users must coordinate with the IMO for VPN configuration.

(4) Direct Dial-up services. Remote Access Service (RAS) and Terminal Services Access Control Server (TSACS) allow users to dial-in and remotely access the FCCS and NIPRNet respectively. These services will be provided to users on an exception basis where a mission requirement exists. Machines used for RAS and TSACS must meet all security requirements in paragraph (1)(c) above.

5. Use of Public Key Infrastructure (PKI) Certificates

a. Public Key Infrastructure (PKI) is an IT infrastructure that enables users to securely and privately secure data. PKI enables the use of encryption, digital signature, and access authentication services in a consistent manner across a wide variety of applications. It provides the following functions:

(1) Authentication: proof the sender is who they claim to be. (public/private key)

(2) Confidentiality: assurance the person receiving is the intended recipient. (encrypt/ decrypt)

(3) Data Integrity: verification that no unauthorized modification of data has occurred. (hash)

(4) Non-Repudiation: assurance for the legal community that the person sending cannot deny participation. (digital signature)

b. PKI is a public key cryptographic system. Three DOD PKI certificates, containing private and public keys are loaded on a Common Access Card (CAC). These certificates allow the user to provide digital identification, sign E-mail, and encrypt E-mail. In this system, two keys are generated for each function. One of these keys is kept private, and is hence termed the private key.

c. The private key is:

(1) Protected by the owner

(2) Used to sign messages

(3) Used to decrypt messages

(4) Kept in physical possession of owner

d. The other key is widely published and is termed the public key. It is:

(1) Distributed freely and openly

(2) Used to verify signatures

(3) Used to encrypt messages

(4) Stored in the user's Contacts folder

(5) Available through the Internet

e. Soft certificates. Currently "soft" (software) for FORSCOM personnel are limited to Army Senior Leadership (General Officers, Senior Executives, and selected senior staff members) and are used to digitally sign and encrypt E-mail messages.

f. The CAC is the new DOD ID card. It is a "hard" certificate and is more than just an ID. It contains computer chip, barcodes, and a magnetic stripe which allow it to be used to:

(1) Access buildings and controlled spaces.

(2) Login to computer systems and networks.

(3) Digitally sign and encrypt E-mail messages

g. Rules for Signing and Encrypting E-mail. E-mail must be encrypted if it contains Sensitive information (e.g., FOUO) or information protected by The Privacy Act of 1974 or The Health Insurance Portability and Accountability Act (HIPPA). Sending digitally-signed E-mail shall be used whenever E-mail is considered Official Business and/or contains Sensitive information. Receiving Encrypted E-mail that is received in encrypted form must be stored in encrypted form if it is retained.

h. Steps for sending digitally-signed messages.

(1) From Outlook. Click New Message button.

(2) TO: address can be from Global, Personal or Contacts addresses.

(3) Type message. To Digitally Sign the message, select the Red Ribbon icon button in the toolbar.

(4) Click Send. If prompted, enter the CAC PIN to send the email. Click OK.

(5) Red Ribbon seal will appear on the envelope of sent messages (check Sent Items to confirm).

(6) Sender must have CAC in the card reader to send signed messages.

i. Steps for sending encrypted messages.

(1) From Outlook. Click New Message button.

(2) Address and compose the message.

(3) Before sending, select the Blue Lock icon. If this icon is not visible, click Encrypt message content and attachments under File -> Properties -> Security.

(4) Click Send. The Blue Lock icon appears on the sent message's envelope.

(5) If this fails contact the FCCS Help Desk for assistance.

j. Steps for opening encrypted messages.

(1) From Outlook - Double click to Open Mail Message

(2) Encrypted messages have a Blue Lock symbol on their envelope icon. Only intended recipients with working PKI can open and read encrypted messages.

(3) Insert your CAC into the card reader.

(4) When you attempt to open an encrypted message, you'll be prompted for your PIN.

(5) Enter your PIN and click OK to read your message.

k. If you have a PKI certificate installed on your computer (for example: software token), you are responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, you should notify your IMO and the issuing Trusted Agent or local registration authority.

6. Computer Security

a. What is the threat?

(1) Threats to your computer and the FCCS can come from a virus, worm, hacker, or even from a disgruntled soldier or DOD civilian in the military or US Government.

(2) Viruses and worms are programs that corrupt and damage programs, data, or both. A program does not have to perform malicious actions to be a virus or a worm; it only needs to infect or alter other programs. Most viruses, however, perform malicious actions, such as deleting data from your hard drive. Worms and viruses may leave one or more programs on your computer called "backdoors" that would allow a hacker free access to your data or use your computer as a "host" from which to infect other computers. Hackers routinely attempt to exploit these backdoors to find further security vulnerabilities and burrow deeper into a network.

(3) Opening an infected e-mail message or attachment from an unknown source is the most common method viruses are spread today. Many viruses are programmed to send emails such that the "from" and "to" addresses are randomly selected from the infected user's contacts or address lists. So even if you know the sender, do not open an attachment in a message until you have confirmed (s)he actually sent it. Unusually terse or nonsensical subject or email text should raise your suspicions about the content of an attachment. To maintain security, do not configure your computer to automatically preview e-mail messages.

(4) Virus-hoax warnings are also common. Many virus and e-mail hoaxes use fake technical or emotional language and include suggestions to delete valid files or take other unnecessary actions. They often provide an "urgent" warning to pass along information to protect everyone from a devastating virus. If you question the validity of a virus warning, check with the FCCS help desk or go to one of the common anti-virus vendor websites which track hoax virus warnings.

(5) Loading unauthorized software, such as "Weather Bug," "Hot Bar," "Google Search," etc. can introduce ad ware, spyware or Trojan horse software to your computer. Not only does this software affect the performance of the system, it puts the network at risk and may even compromise government data.

(6) Improper configuration, whether of the operating system or of authorized applications, can also put the system at risk. An example of improper configuration would be sharing a directory on your workstation without applying proper access controls. Changing Internet Explorer, Outlook or Office security configuration setting also opens the system for compromise.

(7) Deliberately introducing "malicious logic" (the technical term for viruses and other malicious programs) into any Government information system is a violation of a lawful general order under the Uniform Code of Military Justice (UCMJ), Article 92. Personnel not subject to the UCMJ may be subject to adverse action under the United States Code or Federal regulations. In addition to potential punishment under federal law, any such act will result in the immediate revocation of all user network privileges.

(8) The best course of action is to prevent your computer from being infected in the first place. In the FCCS, there are five things users can do to ensure their computer and information are adequately protected:

(a) Ensure the antivirus software on your computer is current. The FCCS policy requires that your computer's antivirus software be updated at least once a week. Antivirus software must also be updated on all personal and Government-owned personal digital assistants (PDAs) and personal electronic devices (PEDs) and any other devices (such as dial-in personal computers) that connect to the network. In many organizations antivirus updates are automatically "pushed" to computers on the network through auto-update software. Note that laptops and other devices which do not routinely reside on the network will not receive these auto-updates. In that case it is the user's responsibility to ensure anti-virus software is up to date. Soldiers and DOD civilians are eligible for free antivirus software for their personal computers. Your IMO or the FCCS Help Desk can provide a copy of this software.

(b) Be aware of and report any unusual computer activity (paragraph 11.b).

(c) Turn off your computer at the end of the day.

(d) Set your computer to scan "all files" when checking for viruses.

(e) Scan all removable media (for example: disks, CDs, tapes, universal serial bus memory sticks) for malicious software (for example: viruses, worms) before transferring any files or using them on a government computer, IT system, or the FCCS network.

- Go to Start, Programs, Symantec Client Security, and select computer scan and select what devices you want to scan.

(9) Even when taking the best precautions, viruses can still occur. There is a period of vulnerability between the time the virus is released on the internet and the time anti-virus vendors identify it and produce signature files. New viruses may be difficult to detect. Here are some symptoms that may indicate the presence of a virus:

(a) Abnormal displays or banners appear on the computer screen.

(b) The computer's performance slows down.

(c) The computer shows unusual activity or displays error messages, file sizes change, or data or programs are lost.

(10) IMMEDIATE ACTION DRILL FOR VIRUSES: If you believe your computer is infected with a virus or worm or is behaving strangely, immediately take the following steps:

(a) Do not turn off your computer.

(b) Disconnect the network cable (which looks like a telephone cable) from the computer.

(c) Call the Help Desk, IASO or IMO

(11) Malicious logic is not the only threat to government information. Much information can be gleaned from small bits of unclassified data available to the general public. Operations Security (OPSEC) is critical to protect DOD information. An emerging threat to OPSEC can be found on commercial Blog sites. Information on these sites is indexed and published to the entire Internet. DOD employees should never write about any official-related activities or information on these sites. AKO provides various forums allowing users to share official information with other authorized users.

(a) Reporting Computer Security Incidents

(12) If you think you have observed a computer security incident, you must report it to your IMO, Help Desk, or IASO immediately. A computer security incident is the act of violating an explicit or implied computer security policy. A few examples of computer security incidents are as follows:

(a) Attempts (either failed or successful) to gain unauthorized access to a system or its data (for example: hacking). Attempts (either failed or successful) to defeat or circumvent computer-network or security controls (for example: SmartFilter, passwords, etc.).

(b) Downloading MP3 files or other unauthorized software.

(c) Writing or knowingly transmitting a virus, worm, or other form of malicious logic.

(d) Forwarding chain e-mail messages.

(13) Additionally, immediately inform the Help Desk, your IMO or IASO if you think—

(a) Your computer has a virus.

(b) Your computer has been hacked or is being hacked.

(c) An authorized or required activity on the network is not functioning correctly.

(14) If you believe your computer is infected with a virus or worm or is behaving strangely, immediately take the following steps:

(a) Do not turn off your computer.

(b) Disconnect the network cable (which looks like a telephone cable) from the computer.

(c) Call the IMO, Help Desk, or IASO.

7. How to Treat Your Government Computer

a. You must treat your computer with care for it to function properly.

(a) Use care when you eat or drink near your computer. Spilling soft drinks, coffee, or other liquids on your computer can damage it and destroy your files.

(b) Keep your system clean and free of dust.

(c) Never disconnect your computer from its network-connection box (unless you think it is infected).

(d) Do not move your computer unless supervised by your IMO or IASO.

(e) Do not expose your computer to extreme heat, cold, or humidity.

(f) Turn off your computer off at the end of the duty day. If your computer is turned off, it can't be attacked from the network. Occasionally users will be asked to log out and leave their systems on overnight so critical IAVA patches can be applied with less interruption of work during the day.

(g) Security patches are pushed to all network-connected systems. Many patches are pushed silently, with minimal impact on users. Some of these updates require a reboot. Users will be warned prior to an automatic reboot, and may normally delay the installation twice before being forced to install and reboot. Occasionally a patch will be critical enough that the installation delay will offered will be short. Users will be warned by a broadcast email message when new security pushes are implemented.

8. Computer-User Test

a. Now that you have read and studied this guide, you are ready to take the Computer User Security Training. After receiving the HQ FORSCOM Form 650-E from your IMO, the FCCS IASO will assign you a temporary password providing you limited access for five working days; the account will be locked after this period. Log on to the network, then register for the Computer User Security Training (IA Awareness Training) link and follow the instructions at https://ia.gordon.army.mil/test/iau/register.asp?org=HQFORSCOM&scorerpt=iaso-g6@forscom.army.mil .

b. Once you have taken and passed the test, the results will be forwarded to the FCCS IASO who will grant you access to operate on the FCCS network. Your access is valid for three (3) years. Because security practices are updated based on the threat, we will ask you to re-familiarize yourself with updated procedures and retest every three years should you continue to need access to the FCCS network.

c. Before you receive a log-on name and password for your computer, your IMO or IASO will require you to read and sign the Computer-User Agreement (Appendix A). Your signature acknowledges your understanding of and agreement to support Army and FCCS policy on the use of computers. Your signature also makes you accountable for every transaction that occurs on your computer account. If you refuse to sign, you will not be given access to the FCCS network.

d. Anytime you use the FCCS, you are responsible for protecting your computer and the network from threat by following proper procedures. This guide will be updated as new threats emerge and computer-network defense tactics, techniques, and procedures change. We encourage you to review this manual often. Further, we will promulgate periodic notices to users advising of them of new requirements or procedures based on updated threat and vulnerability assessments. You are responsible for following those procedures.

9. Conclusion

a. As a computer user, you play a key role in protecting the integrity, availability, and confidentiality of data in the FCCS network. Taking the steps listed above will help you ensure that your computer and all networks to which your computer is connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the command and all DOD agencies that rely on the NIPR and SIPR networks. To summarize:

(1) Guard your password.

(2) Ensure your antivirus software is up-to-date.

(3) Follow the rules on personal use of your computer.

(4) Report viruses and all other network-security incidents to the Help Desk, IMO, or IASO.

Appendix A —
Computer-User Agreement

This appendix is a copy of the Computer-User Agreement on the FORSCOM Command and Control System (FCCS) Automation Training Program Web page at TBP. Your Information Management Officer (IMO) or Information Assurance Security Officer (IASO) will ask you to sign a copy of this agreement before issuing you a password. A copy of the signed user's agreement will be obtained by FORSCOM IASO.

As a user of an information system in FCCS, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any software or install hardware on any Government computer (for example: client-workstation, server) without first getting written approval from the DAA, IMO, or IASO.
3. I will not load any software onto my computer, Government information technology (IT) system, or network without the approval of the DAA, IMO, or IASO.
4. I will not try to access data or use operating systems or programs, except as specifically authorized.
5. Once issued a userid and password:

    a. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will change it or report it to my IMO.

    b. If I have a classified account, I will ensure that my password is changed at least once every 90 days or if compromised, whichever occurs first.

    c. If I have an unclassified account, I will ensure that my password is changed at least once every 150 days or if compromised, whichever occurs first.

    d. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.

    e. I am responsible for all activity that occurs on my individual account, once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.

    f. I understand that if my password does not meet current FCCS standards, I am to change it immediately.

    g. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or magnetic or electronic media.

    h. I will not tamper with my computer to avoid complying with FCCS password policy.

    i. I will never leave my classified computer unattended while I am logged on unless the computer is protected by a "password protected" screensaver.

6. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.
7. I understand that when connected to the Secure Internet Protocol Router Network (SIPRNet), my system operates at the US Secret "system-high" mode. I am responsible for ensuring no uncleared individual has access to my SIPR equipment or the information on the SIPR network. I understand a breach of security on the SIPRnet can potentially threaten any agency on DOD and that compromise of the SIPRnet has the potential to significantly damage US National Security.

    a. Any removable media used on the SIPRnet must be marked and protected immediately according to AR 380-5. In other words, any media inserted into a Secret system is considered Secret and must be handled accordingly.

    b. Removable media (disks, thumb-drives, or compact disks) may not be removed from the office area without the approval of the local commander or head of the organization.

    c. I must protect all material printed from the SIPRNet at the Secret level until the information is downgraded or declassified.

    d. I will not enter information into a system if the information has a higher classification than that for which the system is accredited.

    e. If connected to the SIPRNet, only I will ensure individuals without a proper security clearance and need-to-know are NOT allowed unescorted access to the system.

    f. I will not permit individuals without a US Secret Clearance access to a SIPRNet terminal.

8. I understand TEMPEST regulations require physical separation between classified and unclassified system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the IMO or IASO.
9. I will scan all removable media (for example: disks, CDs, tapes, universal serial bus memory sticks) for malicious software (for example: viruses, worms) before using it on a computer, IT system, or FCCS network.

10. I will not transfer any information between the NIPRNet and SIPRNet without prior written approval. This includes physical transfer of data using removable media (floppy disk, thumb drive, etc.) and manually typing data to copy it from one network to the other.
11. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO, IMO or Help Desk and delete the message.
12. I will not run “sniffer” or any hacker-related software on my Government Computer, Government IT system, or network.
13. I will not download file-sharing software (including copyrighted MP3 music and video files), peer-to-peer software, or games onto my computer, Government IT system, or network.
14. I will not connect any personal IT equipment (for example: PEDs and PDAs (such as Palm Pilots), personal computers, digitally enabled devices) to my computer or to any Government network without the written approval of my Designated Approving Authority (DAA) or IASO and IMO.
15. I will ensure that my antivirus software on my computer is updated at least weekly.
16. I will not use commercial Internet “chat” services (for example: America Online, Microsoft Network Instant Messenger, Yahoo) from my computer. If chat service is needed, I will use government-provided systems.
17. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site Help Desk or IMO. I know what constitutes a security incident and know that I must immediately report such incidents to the Help Desk or IMO.
18. I will comply with security guidance issued by my DAA and IASO.
19. If I have a Public Key Infrastructure certificate installed on my computer (for example: software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my IMO and the issuing Trusted Agent of local registration authority.
20. I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, or IASO, I will ensure that all users in my area of responsibility sign this agreement.
21. I know I am subject to disciplinary action if I violate FCCS computer policy. For US personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Federal regulations.

____

22. Computer-User Name
(Typed or Printed):

____

23. Security Officer Name
(Typed or Printed):

____

24. Computer-User Signature:

____

25. Security Officer Signature:

____

26. Date:

____

27. Date:

Appendix B —
Standard Software Loads for Unclassified and Classified Systems

This appendix is the following application software in the standard build for FCCS workstations configured for use on the Unclassified and Classified machines.

1. Unclassified Systems:

- Operating System: Windows XP
- Microsoft Internet Explorer with patches and FORSCOM configuration
- Adobe Reader
- Microsoft Office 2003
- JetForm FormFlow
- WinZip
- Symantec Antivirus
- DBsign WebSigner
- ActivCard Gold or NetSign for CAC
- Any Critical updates to WIN2K or XP, and Office 2K,XP or 2K3

2. Classified Systems:

- Acrobat Reader
- C2PC
- CMP
- COGNOS Impromptu
- Hummingbird Exceed
- JetForm FormFlow-client
- JMPS
- MADCAP Integration Management Issue (MIMI) (RAPTOR)
- Microsoft Office 2000 (GCCS)
- Microsoft Office 2003 (SIPRNet Only)
- Mozilla and Microsoft Internet Explorer (GCCS)
- Microsoft Internet Explorer (SIPRNet Only)
- Symantec Antivirus
- NT Configuration Files (GCCS)

Appendix C —
FCCS Training Courses Offered

FCCS provides effective software and technology training and resources to all employees of the Forts McPherson/Gillem communities while enhancing employee's job performance to meet FORSCOM local and worldwide operational commitments.

- Defense Travel System
- Automated Message Handling System
- Global Command and Control System – Army Capability Package 1
- G6 FCCS Technical Library

GLOSSARY

SECTION I
Abbreviations

AKO	Army Knowledge Online
AOL	America Online
CD	compact disk
DAA	Designated Approving Authority
DOD	Department of Defense
E-MAIL	Electronic Mail
FCCS	FORSCOM Command and Control System
FORSCOM	United States Army Forces Command
IASO	Information Assurance Security Officer
IAVA	Information Assurance Vulnerability Alert
IMO	Information Management Officer
ISP	Internet service provider
IT	Information Technology
JER	Joint Ethics Regulation
LAN	Local Area Network
MPEG	Moving Picture Experts Group
MSN	Microsoft Network
PDA	personal digital assistant
PED	personal electronic device
PKI	Public Key Infrastructure
SA	System Administrator
UCMJ	Uniform Code of Military Justice
USB	universal serial bus
VPN	Virtual Private Network

SECTION II
Terms

Information Technology (IT)
The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

SIPRNet
Secret Internet-Protocol Router Network. The name of DOD's secret-high classified network.

NIPRNet
Nonsecure Internet Protocol Router Network. The name of DOD's unclassified network.